PCT/KR 2004/000621
RO/KR 22.03.2004

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0018051
Application Number

출 원 년 월 일 : 2003년 03월 22일
Date of Application MAR 22, 2003

출 원 인 : 이유영
Applicant(s) LEE YU YOUNG

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2004 년 03 월 22 일

특 허 청
COMMISSIONER

10[redacted]18051 출력 일자: 2004/3/27

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2003.03.22
【발명의 명칭】	N- 차원 정보를 이용한 정보 전송 시스템 및 전송 방법.
【발명의 영문명칭】	Data Transmit System And Transmit Methods By Using N-dimensional Information.
【출원인】	
【성명】	이유영
【출원인코드】	4-2002-044215-1
【발명자】	
【성명】	이유영
【출원인코드】	4-2002-044215-1
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 출원인 이유영 (인)
【수수료】	
【기본출원료】	20 면 39,000 원
【가산출원료】	2 면 6,800 원
【우선권주장료】	0 건 0 원
【심사청구료】	5 항 269,000 원
【합계】	314,800 원
【면제사유】	학생
【면제후 수수료】	0 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 Client System(10)와 Server System(20) 간, 및 Client System(10)와 Client System(10) 간의 데이터 전송 과정에 있어서, N-차원 정보에 기반한 일회용 암호화 알고리즘을 적용한 정보 전송 시스템 및 전송 방법에 관한 것이다.

N-차원 정보의 기본단위 구조인 File_f의 최상위계층 정보인 T_f(100) 정보와, 상기 T_f 정보에 연계된 하위계층 정보인 M_f.n(200) 정보와, 상기 M_f.n 정보에 연계된 하위계층 정보인 B_f(300) 정보로 구성된 File_f 정보 및, 상기 File_f 정보의 집합인 N-차원 정보를 이용하여, Client System(10) 또는 Sever System(20)에서 송수신하고자 하는 정보에 대하여 N-차원 정보에 기반한 암호화 연산과정을 적용함으로서, 중요한 정보를 전송할 때마다 고유한 암호화 알고리즘을 적용할 수 있는 효과를 얻는다.

【대표도】

도 1

【색인어】

THE TOP CODE, THE MIDDLE CODE, THE BOTTOM CODE, N-차원 정보, 암호화 알고리즘.

【명세서】

【발명의 명칭】

N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법. {Data Transmit System And Transmit Methods By Using N-dimensional Information.}

【도면의 간단한 설명】

도1은 본 발명에 따른 N-차원 정보의 기본 단위 정보의 구조도.

도2는 본 발명에 따른 N-차원 정보의 기본 단위 정보의 집합을 도시한 구조도.

도3은 본 발명에 따른 Client / Server System을 나타낸 블럭도..

도4는 본 발명에 따른 Server System의 Client 인증 과정을 나타낸 플로우차트.

도5는 본 발명에 따른 Client System의 인증정보 전송과정을 나타낸 플로우차트.

도6은 본 발명에 따른 암호화알고리즘을 적용한 정보 전송과정을 나타낸 플로우차트.

도면의 주요부호에 대한 간단한 설명

10 : Client System

15 : Processor 16 : Memory

17 : 저장 장치 19 : Transfer Part

20 : Server System

25 : Processor 26 : Memory

27 : DBMS 28 : DB

29 : Transfer Part

11 : 휴대용 저장매체 22 : 생체 인식 단말기

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<16> 본 발명은 유/무선 통신망 상에서의 정보 전송 시스템에 관한 것으로, 특히 N차원 정보를 이용하여 사용자가 전송하고자 하는 정보를 안전하게 송수신하기 위한 정보 전송 시스템 및 전송 방법에 관련된 것이다.

<17> 이하, 종래 기술에 따른 정보 전송 시스템에 대하여 설명하면 다음과 같다.

<18> 현재 사용자가 유/무선 통신망 상에서 정보를 송수신 할 때, 제 3자에 의한 네트워크 감청, 스내핑, 및 IP spoofing 등을 이용한 크래킹으로 인해 발생할 수 있는 ID/Password 유출 및 사용자 간에 교환하는 정보의 유출에 대한 위험이 존재한다. 특히, 암호화되어 전송되는 사용자 인증정보를 획득한 제 3자는, 상기 획득한 암호화된 사용자 인증정보를 인증 서버로 재전송하여 사용자 인증을 받음으로서, 금융이체, 증권거래 등의 부정 사용을 유발할 수 있다. 이때 암호화 과정을 마친 후 전송되는 사용자 인증정보는 제 3자에 의해 획득되어 재전송 될 때에도 인증 서버에 의해 동일한 방식으로 복호화되어 사용자 인증을 해줌으로서 암호화의 목적을 상실하게 된다. 따라서 OTP(One Time Password)기술이 필요하게 되었으며, 현재

주류를 이루는 두 가지 방식인 Time synchronous 방식과 Challenge response 방식을 이용한 OTP 기술이 있다. 상기 Time synchronous 방식을 적용한 OTP 기술의 경우 일회용 패스워드를 생성하기 위한 암호화 변수로 시간을 이용할 경우, 전 세계에 존재하는 시스템을 동일한 시간으로 일원화하여 구축하기 어려운 문제점이 있다. 물론 그리니치 시간을 이용하면 되지만 현실적으로는 시스템 간의 시간 오차, 및 국가별 적용 시간의 상이함 등으로 인한 시스템 적용의 한계가 있다. 더욱 치명적인 문제점은 상기와 같은 시간 오차로 인하여 일회용 패스워드를 1분 단위로 생성하여 인증서버로부터 사용자 인증을 받음에 따라, 전송되는 사용자 인증 정보를 획득한 제 3자가 이를 1분 안에 다른 인증서버로 재전송함으로서 사용자 인증을 받을 수 있는 문제점이 있다. 또한 Challenge response 방식을 적용한 OTP 기술의 경우, 사용자는 일회용 패스워드를 생성하기 위하여 별도의 일회용 패스워드 연산 처리를 위한 연산장치를 구입하여 연산장치를 휴대하거나 다음에 사용할 일회용 패스워드를 암기하고 있어야 하는 불편한 점이 있다. 또한 현재 정보 전송 방식에서 제일 큰 비중을 차지하는 PKI에 기반한 인증서를 이용할 경우에도, 제 3자에 의한 인증서 복사의 위험이 존재한다. 이때 제 3자가 휴대용 저장매체는 그대로 두고, 인증 관련 정보만 복사했을 경우, 사용자는 인증서가 복사된 사실을 알 수 없다. 따라서 사용자는 인증서 분실 신고 및 재발급 신청을 하지 않는 관계로 제 3자에 의한 부정 사용의 위험이 존재한다. 끝으로 사용자의 생체 인식 정보를 이용한 암호화 및 사용자 인증 시스템의 경우, 사용자는 본인의 생체 인식 정보를 이용하기 위해 고가의 생체 인식 단말기를 구입해야하므로 범용적으로 사용하기에는 한계가 존재할 뿐만 아니라, 사용자의 생체 인식 정보가 유출될 경우, 생체 인식 정보에 기반한 모든 보안 시스템이 한 순간에 그 의미를 상실하는 문제점이 존재한다.

【발명이 이루고자 하는 기술적 과제】

<19> 따라서 본 발명은 상기와 같은 문제점을 해결하기 위해 안출한 것으로서, 유/무선 통신망에서 Client 간, Client와 Server간 송/수신하고자 하는 정보에 대하여 N-차원 정보에 기반한 연산 과정을 적용함으로서 일회용 암호화 알고리즘을 적용한 정보를 생성하여 전송함으로서, 수준 높은 보안 상태에서의 정보 교환 및 사용자 인증을 가능하게 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법을 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<20> 도1은 본 발명에 따른 N-차원 정보의 기본 단위 정보를 나타낸 구조도이다.

<21> 상기와 같은 목적을 달성하기 위한 본 발명에 따른 N-차원 정보의 기본 단위정보인 FILE_f는 THE TOP CODE_f(100), THE MIDDLE CODE_f.n(200), THE BOTTOM CODE_f(300)로 구성되는 것을 특징으로 한다.(f : FILE Number, n : 양의정수)

<22> 편의상 상기 THE TOP CODE_f(100)는 T_f로 표시하고, THE MIDDLE CODE_f.n(200)은 M_f.n으로 표시하고, THE BOTTOM CODE_f(300)는 B_f로 표시하기로 정의한다.

<23> 상기 N-차원 정보의 기본 단위 정보의 하나인 FILE_0의 경우, 상기 THE TOP CODE_f(100)는 T_0으로, THE MIDDLE CODE_f.n(200)은 M_0.n으로, THE BOTTOM CODE_f(300)는 B_0으로 상기 정의에 따라 표시할 수 있다.

<24> 상기 T_f 정보는 상기 N-차원 정보의 기본 단위 정보인 FILE_f 정보를 구성하는 최상위 계층 정보로서 컴퓨터, 휴대용 통신 기기, 출입/근태 제어장치 등을 포함하는 기기에 적용된 키보드 또는 키패드 상의 키를 입력할 때 발생하는 코드를 조합한 정보 및 생체 인식 단말기를 이용하여 얻은 생체 인식 정보를 이용하여 구성되는 것을 특징으로 한다. 상기 T_f 정보를 구

성하는데 있어서, 생체 인식 단말기를 보유한 사용자는 생체 인식 정보를 이용하여 상기 T_f 정보를 구성할 수 있고, 생체 인식 단말기를 보유하지 않은 일반 사용자는 키보드 또는 키패드 상의 키 코드를 조합한 정보를 이용하여 상기 T_f 정보를 구성할 수 있다.

<25> 상기 M_f.n 정보는 N-차원 정보의 기본 단위 정보인 FILE_f 정보를 구성하는 최상위계층 정보인 T_f 정보와 최하위계층 정보인 B_f 정보 사이의 중간계층을 형성하는 중간계층 정보로서, 유/무선 통신망에서 Client간, Client와 Server간 송/수신하고자 하는 정보에 대하여 N-차원 정보에 기반한 암호화 알고리즘을 적용하기 위한 변수 정보의 역할을 하는 것을 특징으로 한다. 상기 M_f.n은 M_f.1에서 M_f.n까지 n개의 중간계층 정보로 구성(n:양의정수)된다. 상기 M_f.1은 T_f에 연계된 하위계층 정보이고, M_f.n-1 정보는 M_f.n 정보의 상위계층 정보($n \geq 2$)이다.

<26> 상기 B_f 정보는 N-차원 정보의 기본 단위 정보인 FILE_f 정보를 구성하는 최하위계층 정보이고 상기 M_f.n 정보에 연계된 하위계층 정보로서, 사용자가 그린 그림, 사용자의 서명, 각종 생체인식 정보, 및 키보드/키패드 상의 임의의 키 값을 이용한 조합 정보를 포함한 이용 가능한 모든 형태의 정보로 구성되는 것을 특징으로 한다.

<27> 상기 N차원 정보의 기본 단위 정보인 FILE_f 정보는 최상위계층 정보인 T_f 정보, 상기 T_f 정보에 연계된 하위계층 정보인 M_f.n 정보, 및 상기 M_f.n 정보에 연계된 하위계층 정보인 B_f 정보로 구성되는 것을 특징으로 한다.

<28> 도2는 본 발명에 따른 N-차원 정보의 기본 단위 정보를 N개 생성하여 구성된 N-차원 정보를 도시한 구조도로서, 상기 N-차원 정보는 휴대용 저장매체 또는 저장장치에 저장되는 것을 특징으로 한다.

<29> 도3은 본 발명에 따른 Client System(10)과 Server System(20)을 나타낸 도면으로, 상세한 내용을 하기에 서술하면 다음과 같다.

<30> 상기 Client System(10)은 퍼스널 컴퓨터, 휴대폰, PDA, 및 스마트폰 등을 포함하는 유/무선 통신 기능이 내장된 Network System 성격의 단말기와 출입/근태제어 단말기와 같은 Local System 성격의 단말기를 모두 포함하며, 상기 Server System(20)은 은행, 증권사 등을 포함하는 금융기관 및 인증센터의 Server를 의미한다.

<31> 상기와 같은 목적을 달성하기 위한 본 발명에 따른 상기 Client System(10)의 특징은 Client System의 기능을 총괄 제어하는 Processor(15)와 상기 Processor에 연결되어 활성화된 정보를 저장하는 Memory(16)와 상기 Processor에 연결되어 N-차원 정보를 저장할 수 있는 저장장치(17)와 상기 Processor에 연결되어 정보를 송수신하는 Transfer Part(19)를 포함하여 구성되는 것을 특징으로 하고, 상기 Server System(20)의 특징은 Server System의 기능을 총괄 제어하는 Processor(25)와 상기 Processor에 연결되어 활성화된 정보를 저장하는 Memory(26)와 상기 Processor에 연결되어 DataBase를 관리하는 DBMS(27)와 상기 Processor에 연결되어 N-차원 정보를 저장할 수 있는 DB(28)와 상기 Processor에 연결되어 정보를 송수신하는 Transfer Part(29)를 포함하여 구성되는 것을 특징으로 한다.

<32> 상기 Client System(10) 및 Server System(20)은 휴대용 저장매체(11) 또는 생체인식 단말기(22)와 연결되는 것을 또 다른 특징으로 한다.

<33> 상기 Client System(10) 및 Server System(20)의 Processor(15,25)의 특징은 N-차원 정보의 T_f(100) 조합정보를 송수신 하는 단계와, N-차원 정보의 T_f(100)조합정보를 System에 마련된 키보드 또는 키패드 또는 생체인식 단말기(22)로부터 입력받는 단계와, 상기 송수신 또는 입력된 N-차원 정보의 T_f(100) 조합정보에 연계된 하위계층 정보인 M_f.1(200) 조합정보를

검색하는 단계와, 상기 검색된 M_f.1(200) 조합정보에 연계된 하위계층 정보인 M_f.n(200) 조합정보(n≥2)를 검색하는 단계와, 상기 검색된 M_f.n(200) 조합정보에 연계된 하위계층 정보인 B_f(300) 조합정보를 검색하는 단계와, 상기 송수신 또는 입력된 T_f(100) 조합정보에 연계된 하위계층 정보인 B_f(300) 조합정보를 검색하는 단계와, 상기 검색한 B_f(300) 조합정보에 상기 검색한 M_f.n 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하는 단계와, 송신하고자 하는 정보에 상기 검색한 M_f.n 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하는 단계와, 수신한 정보에 상기 검색한 M_f.n 조합정보를 변수로 이용하는 복호화 연산과정을 적용한 정보를 생성하는 단계를 포함하여 구성되는 것을 특징으로 하다. 한편 상기 서술한 내용을 바탕으로 상기 Processor(15,25)는 송수신 또는 입력된 M_f.n(200) 정보를 이용하여 검색된 상위계층 정보인 T_f(100) 정보를 암호화 및 복호화 연산을 위한 변수정보로 이용할 수 있는 B_f(300) 정보에 연계된 상위계층 정보인 M_f.n(200) 정보를 검색 단계와, M_f.n(200) 정보에 연계된 상위계층 정보인 T_f(100) 정보를 검색하는 단계 등을 포함하여 구성되는 것을 또 다른 특징으로 한다.

34> 상기 암호화 및 복호화 연산과정은 전송하고자 하는 정보에 N-차원 정보의 T_f(100) 조합정보 또는 M_f.n(200) 조합정보를 변수로 이용한 Octet 단위 치환 연산, Bit 단위 치환 연산 및, 특정 함수를 적용한 연산과정을 적용하는 것을 특징으로 한다.

35> 상기 Client System(10)에 있어서, 상기 Memory(16)는 N-차원 정보를 검색한 정보 및, N-차원 정보를 이용한 연산 정보를 저장하는 것을 특징으로 하고, 상기 저장장치(17)는 Hard Disk와 같은 고정 저장 장치로서 N-차원 정보를 저장하는 것을 특징으로 하고, 상기 Transfer Part(19)는 N-차원 정보의 T_f 정보와 N-차원 정보를 이용한 연산과정이 완료된 정보를 송수신하는 것을 특징으로 한다.

<36> 상기 Server System(20)에 있어서 상기 Memory(26)는 N-차원 정보를 검색한 정보 및, N-차원 정보를 이용한 연산 정보를 저장하는 것을 특징으로 하고, 상기 DBMS(27)은 N-차원 정보가 저장된 DB를 관리하는 것을 특징으로 하고, 상기 DB(28)는 N-차원 정보를 저장하는 것을 특징으로 하고, 상기 Transfer Part(29)는 N-차원 정보의 T_f(100) 정보 또는 M_f.n(200) 정보를 송신하고 N-차원 정보를 이용한 연산과정이 완료된 정보를 수신하는 것을 특징으로 한다.

<37> 상기 휴대용 저장 매체(11)는 정보를 저장할 수 있는 메모리를 내장한 USB포트 연결용 메모리, 메모리스틱, 및 IC Chip 등을 포함하는 휴대 간편한 모든 형태의 휴대용 저장매체로서, N-차원 정보를 저장하는 것을 특징으로 한다.

<38> 상기 생체인식 단말기(22)는 지문, 홍채, 정맥, 얼굴, 음성 등을 포함하는 사용자의 생체인식 정보를 추출할 수 있는 장비로서, N-차원 정보의 T_f 정보를 생체인식 정보로 등록한 사용자의 생체인식 정보를 추출하는 것을 특징으로 한다.

<39> 상기 Client System(10)의 또 다른 특징은 N-차원 정보의 T_f 정보로 구성된 조합정보를 송신하는 단계와, T_f 정보로 구성된 조합정보를 수신하는 단계와, 상기 수신한 T_f 정보에 연계된 하위계층 정보인 M_f.n 정보를 검색하는 단계와, 상기 검색한 M_f.n 정보에 연계된 하위계층 정보인 B_f 정보를 검색하는 단계와, 사용자가 Client System의 키보드 또는 키패드 또는 생체인식 단말기를 이용하여 입력한 T_f 정보에 연계된 하위계층 정보인 B_f 정보를 검색하는 단계와, 사용자가 전송하고자 하는 정보에 상기 검색한 M_f.n 정보를 변수로 이용한 Octet 단위 치환 연산, Bit 단위 치환 연산 및, 특정 함수 적용 등을 포함하는 암호화 연산과정을 적용한 정보를 생성하여 전송하는 단계와, 수신된 정보에 상기 검색한 M_f.n 정보를 변수로 이용한 Octet 단위 치환 연산, Bit 단위 치환 연산 및, 특정 함수 적용 등을 포함하는 복호화 연산과정을 적용한 정보를 생성하는 단계를 포함하여 구성되는 것을 또 다른 특징으로 한다.

<40> 상기 Server System(20)의 또 다른 특징은 N-차원 정보의 T_f(100) 정보로 구성된 조합 정보를 송신하는 단계와, 상기 송신한 T_f 정보에 연계된 하위계층 정보인 M_f.n 정보를 검색하는 단계와, Client가 등록한 인증정보를 검색하는 단계와, 상기 검색한 인증정보에 상기 검색한 M_f.n 정보를 변수로 이용한 Octet 단위 치환 연산, Bit 단위 치환 연산 및, 특정 함수 적용 등을 포함하는 암호화 연산과정을 적용한 정보를 생성하는 단계와, Client로부터 인증정보를 수신하는 단계와, 상기 Client로부터 수신한 인증정보와 상기 암호화 연산과정을 적용한 정보를 서로 비교하여 일치할 경우 인증 처리를 하는 단계와, 상기 Client로부터 수신한 인증정보를 상기 검색한 M_f.n 정보를 변수로 이용한 Octet 단위 치환 연산, Bit 단위 치환 연산 및, 특정 함수 적용 등을 포함하는 복호화 연산과정을 적용한 정보를 생성하여 Client가 등록한 인증정보와 서로 비교하여 일치할 경우 인증 처리를 하는 단계를 포함하는 것을 또 다른 특징으로 한다.

<41> 본 발명의 다른 목적, 특징 및 이점들은 첨부한 도면을 참조한 실시예들의 상세한 설명을 통해 명백해질 것이다.

<42> 이하, 본 발명에 따른 Client System(10) 및 Server System(20)의 N-차원 정보를 이용한 정보 전송시스템 및 전송방법의 바람직한 실시예에 대하여 첨부한 도면을 참조하여 설명하면 다음과 같다.

<43> Client System(10)와 Server System(20)간 인증을 위해 Client는 금융기관 또는 인증기관에서 본 발명에 따른 N-차원 정보를 생성하여, Client System(10)의 저장장치(17)와 Server System(20)의 DB(28)와 휴대용 저장매체(11)에 등록및 저장한다.

<44> 도4는 본 발명에 따른 N-차원 정보를 이용한 정보 전송 과정에 대한 일예를 나타낸 플로우차트로서, 특히 Server System(20)에 있어서 Client System(10)에 대한 인증 처리과정을 나타낸 것으로 상세한 내용을 하기에 서술하면 다음과 같다.

<45> (a) N-차원 정보의 T_f(100) 정보를 Random하게 추출하여 조합된 정보를 생성하여 인증을 요청하는 Client System(20)으로 전송하는 단계(S1)와;

<46> (b) 상기(a)단계에서 전송된 T_f(100) 조합정보에 연계된 하위 계층 정보인 M_f.n(200) 조합정보를 검색하는 단계(S2)와;

<47> (c) Client가 등록한 인증정보에 상기(b)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하는 단계(S3)와;

<48> (d) Client로부터 인증정보를 수신하는 단계(S4)와;

<49> (e) 상기(c)단계에서 암호화 연산과정을 적용하여 생성한 정보와 상기(d)단계에서 Client로부터 수신한 인증정보가 서로 일치하는지 분석하는 단계(S5)와;

<50> (f) 상기(e)단계에서 분석결과 서로 일치할 경우(S6) Client에 대한 인증을 처리하고, Client가 요청하는 사항을 처리하는 단계(S7)를 포함하는 N-차원 정보를 이용한 정보 전송방법을 특징으로 한다.

<51> 도5는 본 발명에 따른 N-차원 정보를 이용한 정보 전송 과정에 대한 일예를 나타낸 플로우차트로서, 특히 Client System(10)에 있어서 Server System(20)에 인증을 요청하기 위한 처리과정을 나타낸 것으로 상세한 내용을 하기에 서술하면 다음과 같다.

<52> (g) Server System(20)으로부터 N-차원 정보의 T_f(100) 조합정보를 수신하는 단계(S8)와;

<53> (h) 휴대용 저장매체(11) 또는 저장 장치(17)을 이용하여 상기(g)단계에서 수신한 T_f(100) 조합정보에 연계된 하위 계층 정보인 M_f.n(200) 조합정보를 검색하는 단계(S9)와;

<54> (i) 사용자가 전송하고자 하는 인증정보에 상기(h)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하여 Server System(20)으로 전송하는 단계(S10)를 포함하는 N-차원 정보를 이용한 정보 전송방법을 특징으로 한다.

<55> 서로 다른 Client System(10)와 Client System(10)간 암호화된 정보 전송을 하고자 하는 Client는 본 발명에 따른 N-차원 정보를 생성하여, T_f(100) 정보와 M_f.n(200) 정보를 암호화된 정보를 전송하기 이전에 서로 공유하여 각각의 Client System(10)의 저장 장치(17)와 휴대용 저장매체(11)에 저장한다.

<56> 도6은 본 발명에 따른 N-차원 정보를 이용한 암호화된 정보를 송수신하기 위한 전송 과정에 대한 일예를 나타낸 플로우차트로서, 특히 서로 다른 Client System(10)간에 암호화된 정보를 전송하는 처리과정을 나타낸 것으로 상세한 내용을 하기에 서술하면 다음과 같다.

<57> (j) N-차원 정보의 T_f(100) 정보를 Random하게 추출하여 조합된 정보를 생성및 전송하여 정보를 교환하고자 하는 Client간 공유하는 단계(S11)와;

<58> (k) 상기(j)단계에서 공유한 T_f(100) 조합정보에 연계된 하위 계층 정보인 M_f.n(200) 조합정보를 검색하는 단계(S12)와;

<59> (l) 정보를 송신하는 Client가 송신하고자 하는 정보에 상기(k)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하여 송신하는 단계(S13)와;

<60> (m) 정보를 수신하는 Client가 수신된 정보에 상기(k)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 복호화 연산과정을 적용한 정보를 생성하는 단계(S14)를 포함하는 N-차원 정보를 이용한 정보 전송방법을 특징으로 한다.

【발명의 효과】

<61> 상술한 바와 같이, 본 발명은 Client System(10)와 Server System(20) 간의 인증 처리 과정 및, Client System(10)와 Client System(10) 간의 데이터 전송 과정에 있어서, N-차원 정보에 기반한 T_f(100) 정보와 M_f.n(200) 정보와 B_f(300) 정보를 이용하여, Client System(10) 또는 Sever System(20)에서 전송하고자 하는 정보에 대하여 송수신된 T_f(100) 조합정보에 따른 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산 과정을 적용함으로서, 고유의 암호화 알고리즘을 제공할 수 있는 효과를 제공한다.

【특허청구범위】

【청구항 1】

최상위계층 정보인 T_f(100) 정보와, 상기 T_f 정보에 연계된 중간계층 정보인 M_f.n(200) 정보와, 상기 M_f.n 정보에 연계된 최하위계층 정보인 B_f(300) 정보로 구성되는 것을 특징으로 하는 기본 단위 정보인 File_f 정보와;

상기 File_f 정보로 구성된 집합인 N-차원 정보의 Data 구조; 및,

상기 N-차원 정보의 Data 구조가 저장된 저장매체를 포함하여 구성되는 것을 특징으로 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법.

【청구항 2】

N-차원 정보에 있어서 최상위계층 정보인 T_f(100) 정보는 Client System(10)와 Server System(20)에 마련된 키보드/키패드 또는 각종 생체인식 단말기(22)로부터 생성된 정보로 구성되어, 키보드/키패드 입력에 의해 발생되는 코드정보 또는 생체 인식 단말기로부터 획득되는 Client의 생체 인식정보에 의하여 Access 되어지는 것을 특징으로 하고,

N- 차원 정보에 있어서 중간계층 정보인 M_f.n(200) 정보는 M_f.1 정보에서 M_f.n 정보까지 n차원으로 연계된 중간계층 정보로 구성가능하고, 상기 M_f.1 정보는 N-차원 정보의 최상위계층 정보인 T_f(100)정보에 연계된 하위계층 정보이고, 상기 M_f.n 정보는 상기 B_f(300)정보의 상위계층 정보이고, M_f.n-1 정보는 M_f.n정보의 상위계층 정보로서, N-차원 정보에 기반한 암호화 연산을 위한 변수 정보로 구성되어지는 것을 특징으로 하고,

상기 B_f(300) 정보는 Client가 Server System(20)의 DB(28)에 등록하고자 하는 인증정보로 구성되어지는 것을 특징으로 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법.

【청구항 3】

Server System(20)의 인증 처리과정에 있어서,

(a) N- 차원 정보의 T_f(100) 정보를 Random하게 추출한 조합정보를 생성하여 Client System(20)으로 전송하는 단계와;

(b) 상기(a)단계에서 생성한 T_f(100) 조합정보에 연계된 하위 계층 정보인 M_f.n(200) 조합정보를 검색하는 단계와;

(c) Client 가 등록한 인증정보에 상기(b)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하는 단계와;

(d) 상기(c)단계에서 암호화 연산과정을 적용하여 생성한 정보와 Client로부터 수신한 인증정보가 서로 일치하면 사용자 인증을 승인하는 단계를 포함하여 구성되는 것을 특징으로 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법.

【청구항 4】

Client System(10)의 인증 처리과정에 있어서,

(e) N- 차원 정보의 T_f(100) 조합정보를 수신하는 단계와;

(f) 휴대용 저장매체(11) 또는 저장 장치(17)을 이용하여 상기(e)단계에서 수신한 T_f(100) 조합정보에 연계된 하위계층 정보인 M_f.n(200) 조합정보를 검색하는 단계와;

(g) Client가 전송하고자 하는 인증정보에 상기(f)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하여 Server System(20)으로 전송하는 단계(S10)를 포함하여 구성되는 것을 특징으로 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법.

【청구항 5】

N-차원 정보의 T_f(100) 정보와 M_f.n(200) 정보를 공유한 서로 다른 Client System(10) 간의 암호화된 정보 송수신 과정에 있어서,

(h) N- 차원 정보의 T_f(100) 정보를 Random하게 추출한 조합정보를 공유하는 단계와;

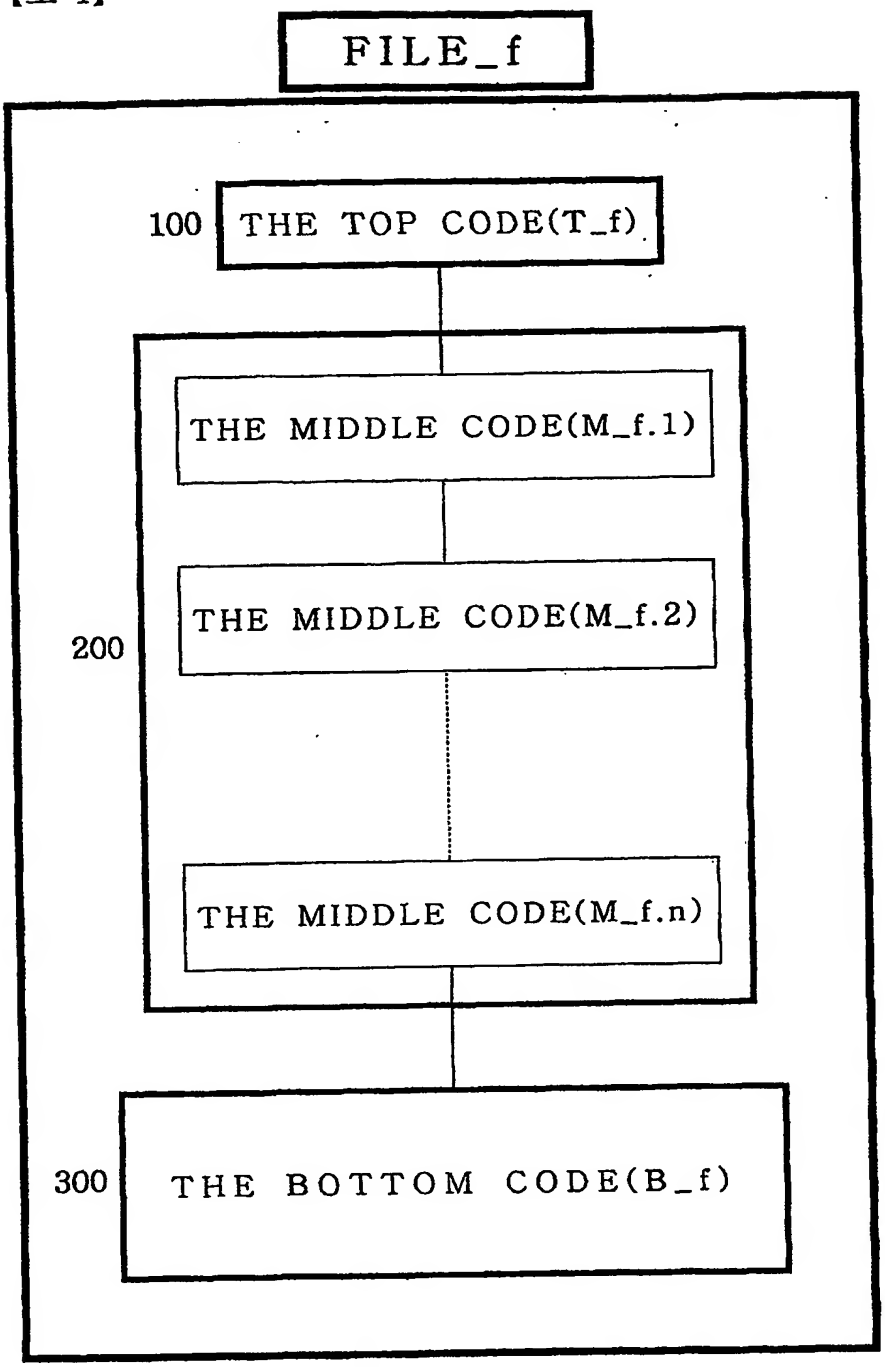
(i) 상기(h)단계에서 공유한 T_f(100) 조합정보에 연계된 하위 계층 정보인 M_f.n(200) 조합정보를 검색하는 단계와;

(j) 정보를 송신하는 Client가 송신하고자 하는 정보에 상기(i)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 암호화 연산과정을 적용한 정보를 생성하여 송신하는 단계와;

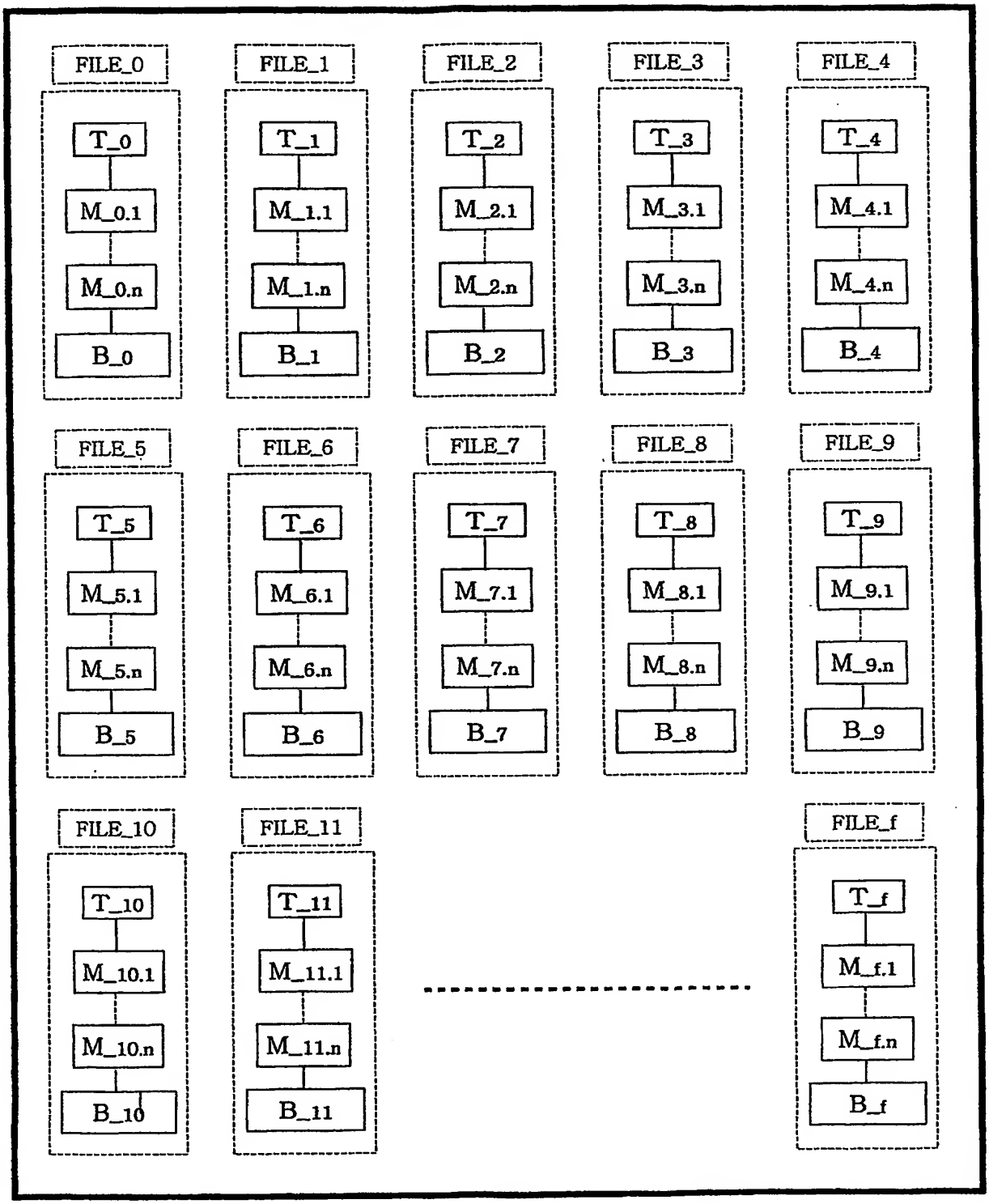
(k) 정보를 수신하는 Client가 수신된 정보에 상기(i)단계에서 검색한 M_f.n(200) 조합정보를 변수로 이용하는 복호화 연산과정을 적용한 정보를 생성하는 단계를 포함하여 구성되는 것을 특징으로 하는 N-차원 정보를 이용한 정보 전송 시스템 및 전송 방법.

【도면】

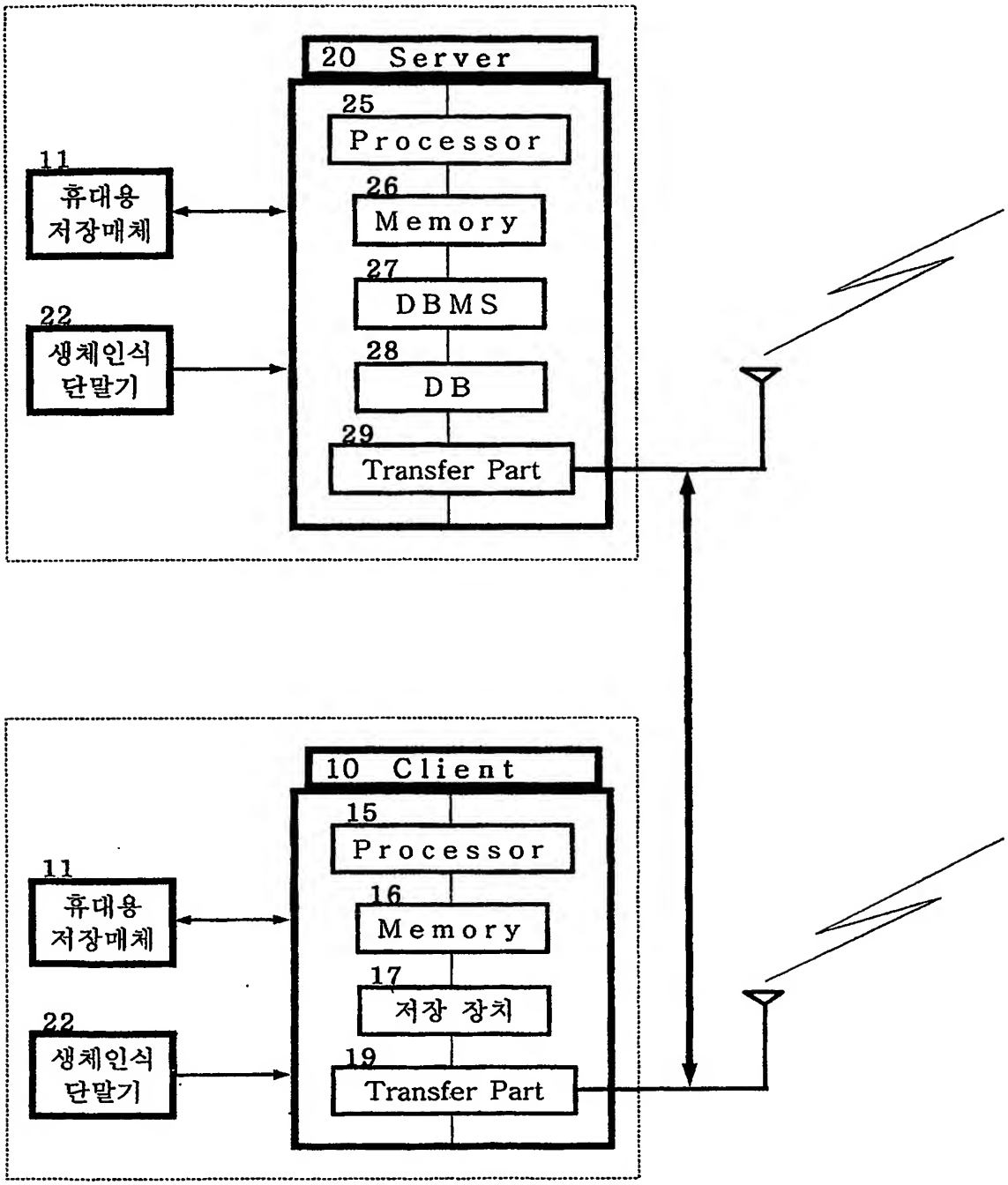
【도 1】


FILE_f
100
THE TOP CODE(T_f)
THE MIDDLE CODE(M_f.1)
200
THE MIDDLE CODE(M_f.2)
THE MIDDLE CODE(M_f.n)
300
THE BOTTOM CODE(B_f)

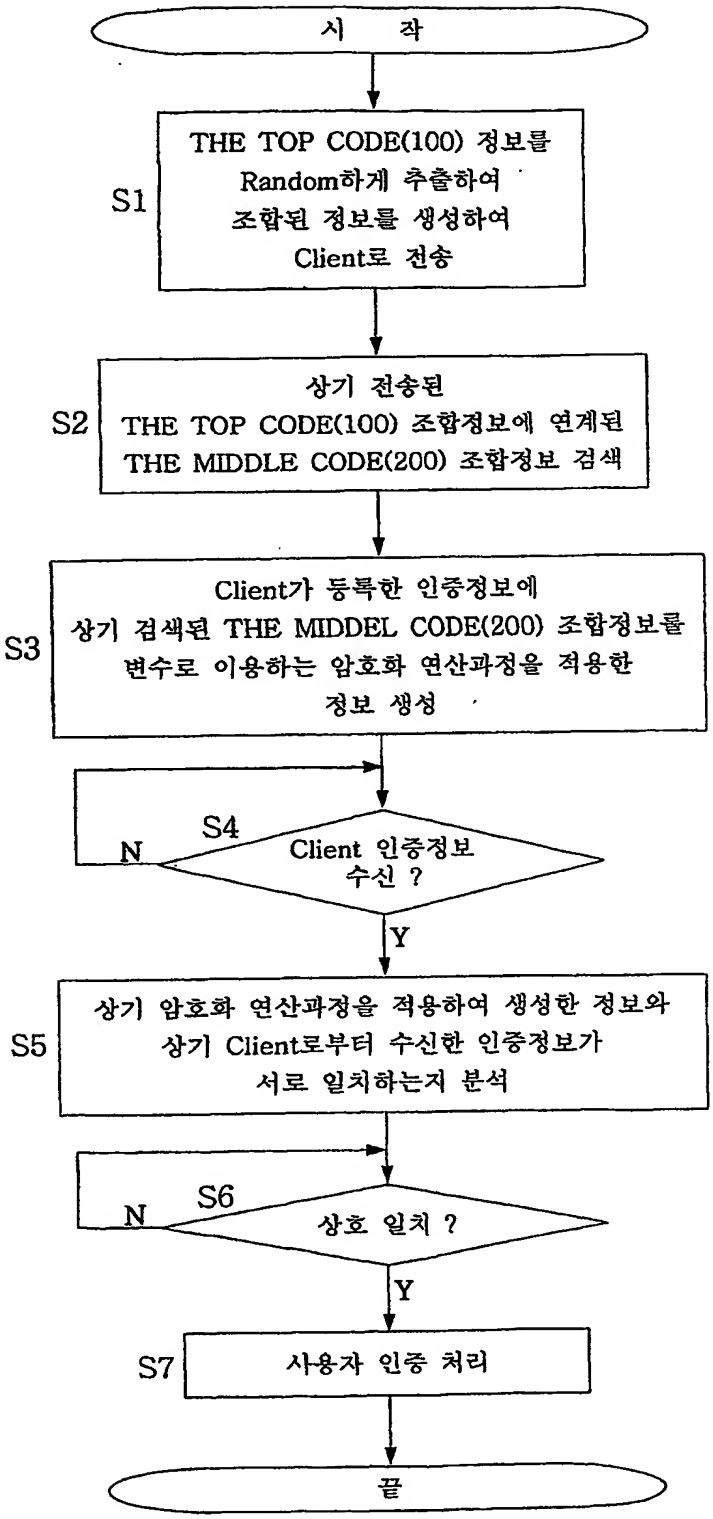
【도 2】


FILE_0
T_0
M_0.1
M_0.n
B_0
FILE_1
T_1
M_1.1
M_1.n
B_1
FILE_2
T_2
M_2.1
M_2.n
B_2
FILE_3
T_3
M_3.1
M_3.n
B_3
FILE_4
T_4
M_4.1
M_4.n
B_4
FILE_5
T_5
M_5.1
M_5.n
B_5
FILE_6
T_6
M_6.1
M_6.n
B_6
FILE_7
T_7
M_7.1
M_7.n
B_7
FILE_8
T_8
M_8.1
M_8.n
B_8
FILE_9
T_9
M_9.1
M_9.n
B_9
FILE_10
T_10
M_10.1
M_10.n
B_10
FILE_11
T_11
M_11.1
M_11.n
B_11
FILE_f
T_f
M_f.1
M_f.n
B_f

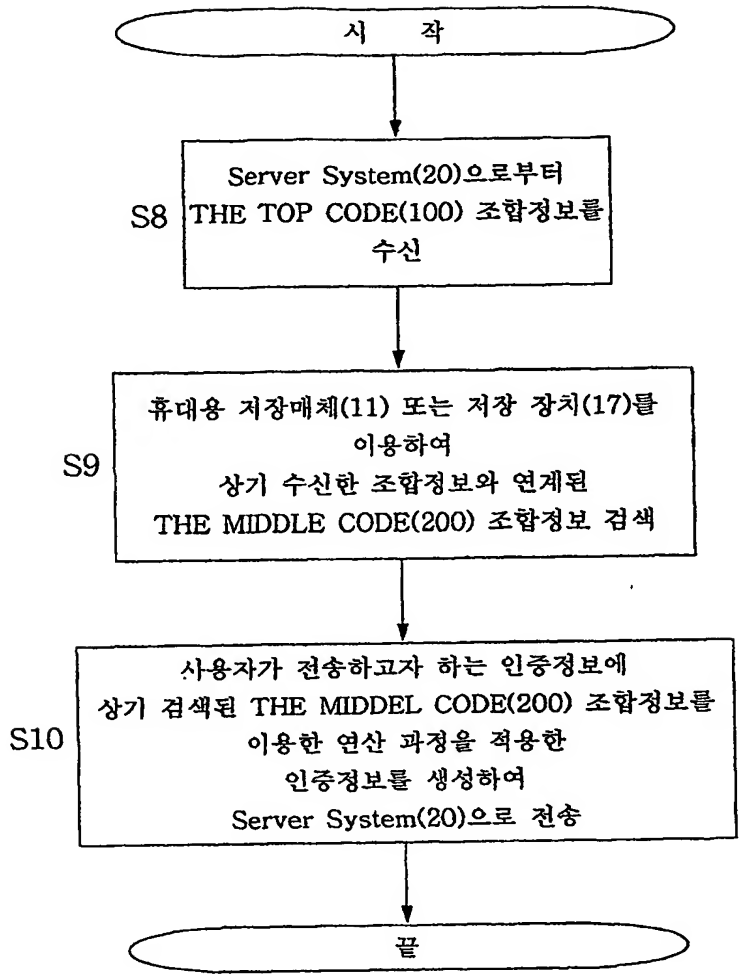
【도 3】


20 Server
25
Processor
26
Memory
27
DBMS
28
DB
29
Transfer Part
11
휴대용 저장매체
22
생체인식 단말기
10 Client
15
Processor
16
Memory
17
저장 장치
19
Transfer Part
11
휴대용 저장매체
22
생체인식 단말기

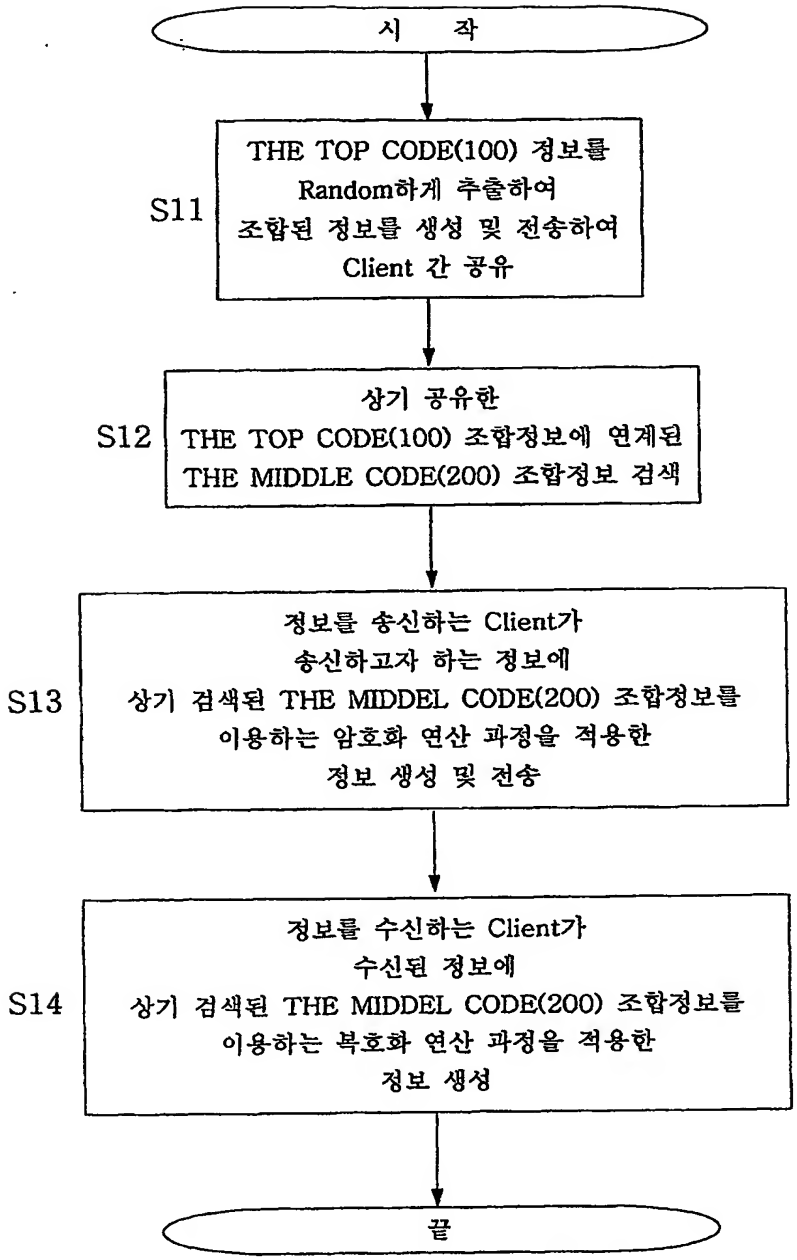
【도 4】


시 작
S1
THE TOP CODE(100) 정보를
Random하게 추출하여
조합된 정보를 생성하여
Client로 전송
S2
상기 전송된
THE TOP CODE(100) 조합정보에 연계된
THE MIDDLE CODE(200) 조합정보 검색
S3
Client가 등록한 인증정보에
상기 검색된 THE MIDDEL CODE(200) 조합정보를
변수로 이용하는 암호화 연산과정을 적용한
정보 생성
S4
N
Client 인증정보
수신 ?
Y
S5
상기 암호화 연산과정을 적용하여 생성한 정보와
상기 Client로부터 수신한 인증정보가
서로 일치하는지 분석
S6
N
상호 일치 ?
Y
S7
사용자 인증 처리
끝

【도 5】


시 작
S8
Server System(20)으로부터
THE TOP CODE(100) 조합정보를
수신
S9
휴대용 저장매체(11) 또는 저장 장치(17)를
이용하여
상기 수신한 조합정보와 연계된
THE MIDDLE CODE(200) 조합정보 검색
S10
사용자가 전송하고자 하는 인증정보에
상기 검색된 THE MIDDEL CODE(200) 조합정보를
이용한 연산 과정을 적용한
인증정보를 생성하여
Server System(20)으로 전송
끝

【도 6】


시 작
S11
THE TOP CODE(100) 정보를
Random하게 추출하여
조합된 정보를 생성 및 전송하여
Client 간 공유
S12
상기 공유한
THE TOP CODE(100) 조합정보에 연계된
THE MIDDLE CODE(200) 조합정보 검색
S13
정보를 송신하는 Client가
송신하고자 하는 정보에
상기 검색된 THE MIDDEL CODE(200) 조합정보를
이용하는 암호화 연산 과정을 적용한
정보 생성 및 전송
S14
정보를 수신하는 Client가
수신된 정보에
상기 검색된 THE MIDDEL CODE(200) 조합정보를
이용하는 복호화 연산 과정을 적용한
정보 생성
끝